DRAFT MOBILE GAMING SYSTEM STANDARDS AND POLICIES

This draft mobile gaming document is intended to provide further clarification on applicable mobile gaming Technical Standards and additionally to define policies associated with the manufacturing and operation of mobile gaming systems. It is important to note that mobile gaming is an extension of the Technical Standards for System Based and System Supported Gaming Devices.

Technical Standard 1.050. Physical Security.

2(a) For the client portion of the system supported game, comply with Technical Standard 1.050(1).

Policy 1.050(2)(a):
System supported mobile gaming clients must:

1. *Actively monitor illegal entry into the device.*
2. *Retain evidence of the entry.*
3. *Render itself unusable for gaming transactions until properly cleared by authorized personnel.*

3(a) For the client portion of the system based game, comply with Technical Standard 1.050(1).

Policy 1.050(3)(a):

System based mobile gaming devices must retain evidence of any illegal entry.

Technical Standard 4.010. User Authorization.

1. Mobile gaming systems must employ a mechanism approved by the Chairman which is capable of verifying that the mobile communications device is being operated by an authorized person.

Policy 4.010(1):

1. *All systems must support and employ strong user authentication, authorization, and accounting that checks against a user database.*
2. *Strong user authentication: Two layers of security – e.g. Username/Password (U/P) & Biometrics, U/P & Hard Token.*
3. *Two layers of security authorization must occur prior to the opening of a session.*

2. The mechanism used to verify that the mobile communications device is being operated by an authorized person must be capable of being initiated both on demand and on a regular basis.

Policy 4.010(2):

1. *Users must be verified at random time increments not to exceed 15 minutes with at least one level of security, e.g. U/P.*
2. *A session is considered closed if user authentication has not been successfully completed within a 15 minute timeframe, the mobile unit has been disabled due to boundary violation, or the user or system has terminated the session.*

3. Authorization information transmitted by the mobile communications device to the mobile gaming system for identification purposes must be collected at the time of the request from the mobile gaming system and may not be stored on the mobile communications device.

4. The Chairman, in his/her sole and absolute discretion, may waive the requirements of this section for mobile communications devices that cannot be reasonably moved by a patron.

Technical Standard 4.020. Mobile Communications Device Communication with a Mobile Gaming System.

1. Communication between a mobile communications device and a mobile gaming system must be conducted using a method that securely links the mobile communications device to the mobile gaming system and authenticates both the mobile communications device and mobile gaming system as authorized to communicate over that link.

Policy 4.020(1) and 1.062(1):

1. *Communications between the server(s) and the mobile client must deploy an SSL/TLS scheme to provide for authentication of the mobile unit and the server, integrity of the data communicated, and for confidentiality by encrypting the data communicated.*
2. *Client and server must be authenticated at least once every five minutes.*
3. *For Wireless 802.1x communications the system must:*
    a. *Employ and encryption standard utilizing a minimum of 128 bits.*
    b. *Not broadcast the SSID.*

    c. *SSID must be changed from their default and must not be made up of information related to the operator (e.g. abccasino) or the type of transactions occurring over the network (e.g. gamingap).*
    d. *Provide physical security for access points.*
    e. *Access points must implement MAC filtering.*
    f. *Mobile device ad hoc modes must be disabled.*
4. *The system must maintain an authorized list of devices which it may communicate with, which must include the device name, a unique device ID and the devices MAC address.*
5. *The system must provide a log of all failed attempts at network access which includes the device name and MAC address.*

2. Mobile gaming system components which interface mobile communications devices must sufficiently isolate the mobile communications devices from the server portion of the mobile gaming system.

Policy 4.020(2):

1. *A firewall must exist between any wireless access points or like device and the gaming server(s).*
2. *The firewall must be hardened network appliance.*

3. A mobile communications device must be designed or programmed such that it may only communicate with authorized mobile gaming systems.

Policy 4.020(3):

Mobile device communications ports must be limited to ports for communication with the gaming system servers only. Other communications such as IR and Bluetooth must be disabled unless specifically used and limited to functions used to comply with a Technical Standard or policy.

Technical Standard 4.030. Location Restrictions. Mobile gaming systems must be designed to restrict the gaming operation of the mobile communications device to public areas as defined by Regulation 5.220.

Policy 4.030:

1. *System must be capable of identifying the location of all active mobile devices within 10 feet of actual location.*
2. *Gaming area coverage may not extend into prohibited areas.*
3. *If a patron enters a nongaming area the system must:*
    a. *Suspend gaming transactions.*

    b. *Notify the patron that the current gaming transaction has been suspended and will be suspended until the patron reenters a gaming area and is reauthorized.*
4. *Upon reentry into a gaming area the patron must be authenticated (Policy 4.010(2)) and the device must return to the last known state prior to gaming activity suspension.*

Technical Standard 4.040. Mobile Communications Device Volume. Mobile communications devices must be capable of adjusting and/or muting the volume on the device.

Additional Mobile Gaming Policies:

1. *Mobile devices must include patron help screens that include the rules associated with the operation of the mobile device.*
2. *Operators must provide mobile gaming operation information to patrons such as gaming area maps, rules of operation, and how to operate.*
3. *System based mobile gaming systems must provide an easily accessible terminal that will allow for the reconciliation of game activity (play history, etc.) on any mobile unit in the case of mobile device failure or disputed games.*